UMU Scan for Symbian OS™
User Manual

25 September 2009
Version 1.4

“UMU Scan” is a registered trademark of UMU Limited and UMU Scan product names and symbols/logos are either trademarks or registered trademarks of UMU Limited. All product names referenced herein are trademarks or registered trademarks of their respective companies. UMU Limited disclaims proprietary interest in the marks and names of others. Although UMU Limited makes every effort to ensure that this information is accurate, UMU Limited will not be liable for any errors or omission of facts contained herein. UMU Limited reserves the right to modify specifications cited in this document without prior notice.

Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of UMU Limited.

Copyright ©2007 - 2009 UMU Limited. All rights reserved.

HOW THIS MANUAL IS ORGANISED **4**

PDF DOCUMENT 4
FOR MORE INFORMATION 4

UMU SCAN FOR SYMBIAN OS™ **5**

KEY FEATURES 5

INSTALLING UMU SCAN FOR SYMBIAN OS™ **6**

USING UMU SCAN FOR SYMBIAN OS™ **6**

Running UMU Scan for Symbian OS™ *6*
Options *9*
Status *11*
Scanning *12*
Quarantine *13*
Updates *14*
Settings *16*
Exiting *21*
Uninstalling *21*

TECHNICAL SUPPORT **22**

IN PROGRAM 22
FREQUENTLY ASKED QUESTIONS 22
EMAIL SUPPORT 22
TELEPHONE SUPPORT 22

ABOUT UMU LIMITED **23**

Figure 1: Activation 6
Figure 2: Enter product key 7
Figure 3: License 7
Figure 4: License details 8
Figure 5: Privacy screen 8
Figure 6: Disable privacy option screen 9
Figure 7: Menu screen 9
Figure 8: Options on the menu screen 10
Figure 9: About screen 10
Figure 10: Status on the menu screen 11
Figure 11: Status screen 11
Figure 12: Scan option 12
Figure 13: Scan screen 12
Figure 14: Scan report screen 13
Figure 15: Quarantine option 13
Figure 16: Quarantine screen 14
Figure 17: Update option 14
Figure 18: Update pop up 15
Figure 19: Update screen 15
Figure 20: Settings option 16
Figure 21: Settings screen 16
Figure 22: Active scan settings screen 17
Figure 23: Scan settings screen 18
Figure 24: Update settings screen 19
Figure 25: Detection settings screen 20
Figure 26: Log settings screen 20
Figure 27: Exit button 21
Figure 28: Help screen 22

How This Manual is Organised

This User Manual is divided into the following chapters:

Introduction: Provides general information about UMU Scan.

Installing UMU Scan: This section gives instructions on installing UMU Scan onto your device.

Using UMU Scan: Describes how to use UMU Scan.

Technical Support: Describes how to get help with using UMU Scan.

About UMU Limited: Describes the company background and products.

PDF Document

This manual is provided in PDF (Portable Document Format). The PDF document can be used for online viewing and printing using Adobe® Acrobat® Reader. When printing the manual, please print the entire manual, including the copyright and disclaimer statements.

For More Information

Visit UMU Limited at http://www.umuglobal.com/ for documentation, training, downloads, and service and support contacts.

In our constant attempts to improve our documentation, we would welcome your feedback. If you have any questions, comments, or suggestions about this or any other UMU document, please contact us at documentation@umuglobal.com.

UMU Scan for Symbian OS™

UMU Scan for Symbian OS™ protects your S60 2nd Edition, S60 3rd Edition or S60 5th Edition device against malicious code attacks.

UMU Scan scans all files on your device both on demand and on access. All infected files are immediately quarantined to protect your device and your data.

To work effectively, antivirus software must be regularly updated with the latest virus definitions. UMU Scan will prompt you to update regularly and can be updated manually through the main menu screen in the program.

Key Features

UMU Scan offers the following key features:

- The program has been designed and created with Symbian OS™ devices in mind so it is compact and efficient.
- Fast efficient scan process.
- Easy to use interface.
- Real time protection of files received via Bluetooth™, MMS, SMS, WiFi, and Infrared.
- User configurable automatic updates.
- Fast, optimised, and secure update process.
- Viruses automatically quarantined.
- On demand scanning of entire device including memory cards.
- Easily installed and uninstalled.

Installing UMU Scan for Symbian OS™

You will be provided with a SIS file. The SIS file can either be installed using the PC Suite or directly on your device. We recommend you run UMU Scan and update the product immediately to ensure you have the most up to date virus definitions.

Using UMU Scan for Symbian OS™

Running UMU Scan for Symbian OS™

Press the Applications key and either scroll down to UMU Scan or choose My Own and scroll down to UMU Scan. Click the icon; this will run UMU Scan and product activation will start.

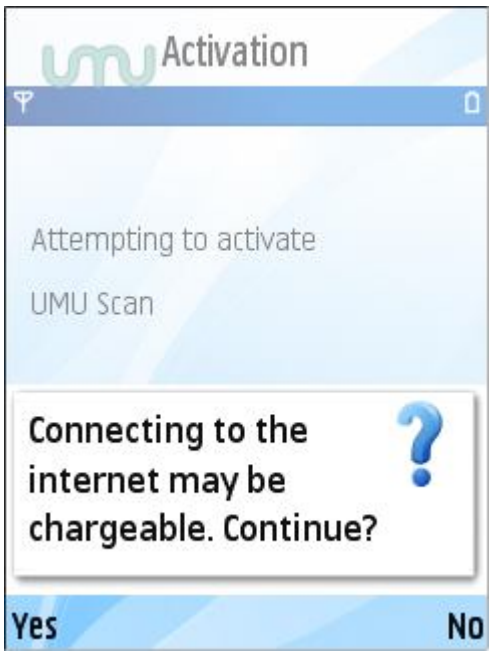

Figure 1: Activation

Next, you will be asked to select a valid access point. You will now be asked to enter your Product Key. If the server has already found your license this step will be bypassed.

Figure 2: Enter product key

Once a valid product key has been entered, you will be asked to accept the license.

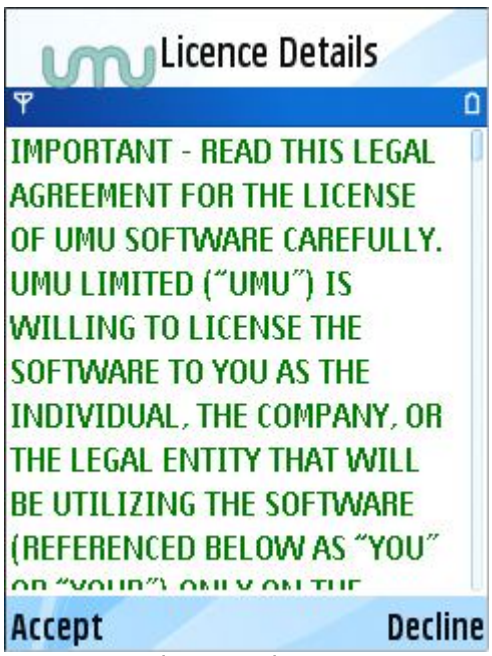

Figure 3: License

Finally, you will be shown your license details.

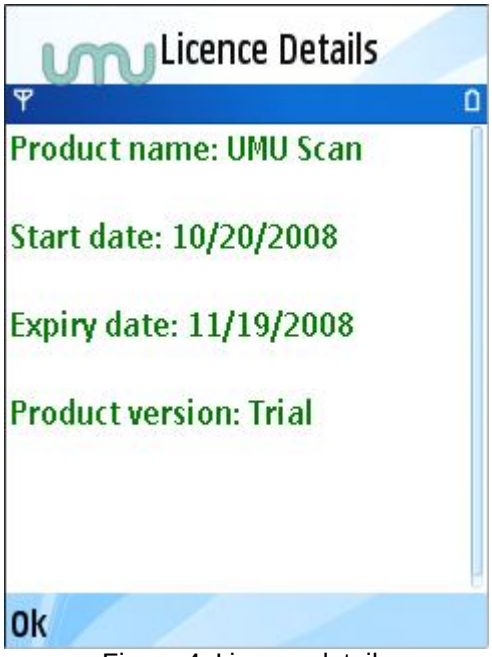

Figure 4: License details

Now activated UMU Scan will start by displaying a privacy statement.

Licence Details
App. mgr.
Web
Go to
For your information
This application will make use of the following features of your phone - Reads and Writes User data on your device.
Making a connection to the internet.
Do you wish to continue using the
Yes
No
Figure 5: Privacy screen

At this point, you have two options:

1. If you choose No, the application will close but will remain installed on your device.

2. If you choose Yes, a second screen is displayed (below) where you can choose whether the first Privacy Screen is displayed every time you open UMU Scan.

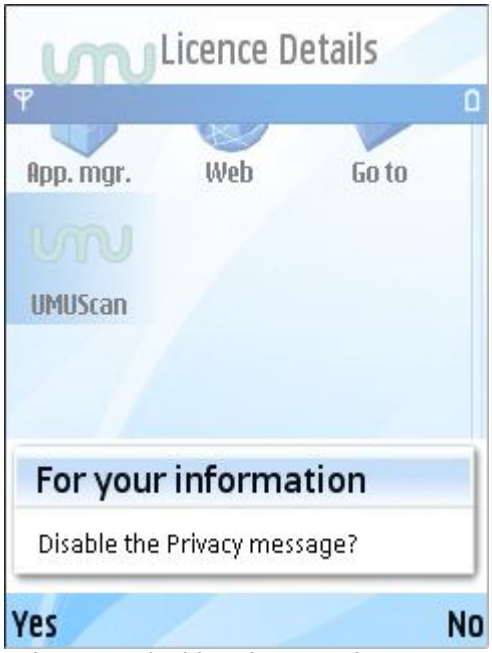

Figure 6: Disable privacy option screen

Once you have made your choices, the welcome screen will appear followed by the menu screen.

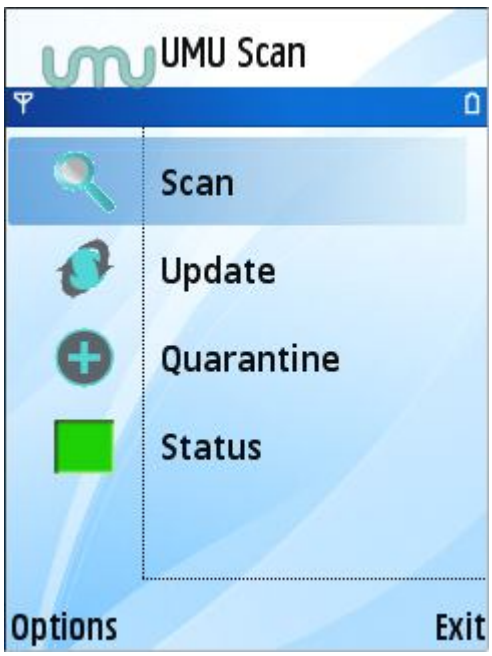

Figure 7: Menu screen

Options

You can find out which version of UMU Scan you have by choosing Options and then About. This also shows you the version of the signature database and how many samples it contains. To exit choose OK and you will return to the screen you were on.

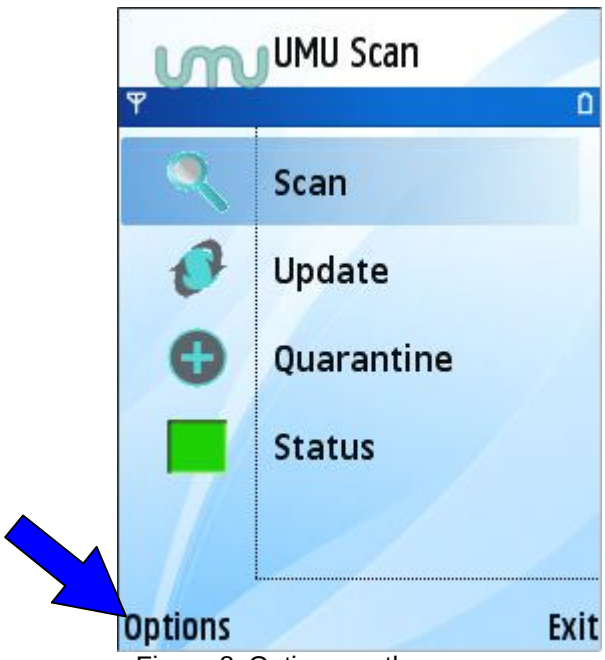

Figure 8: Options on the menu screen

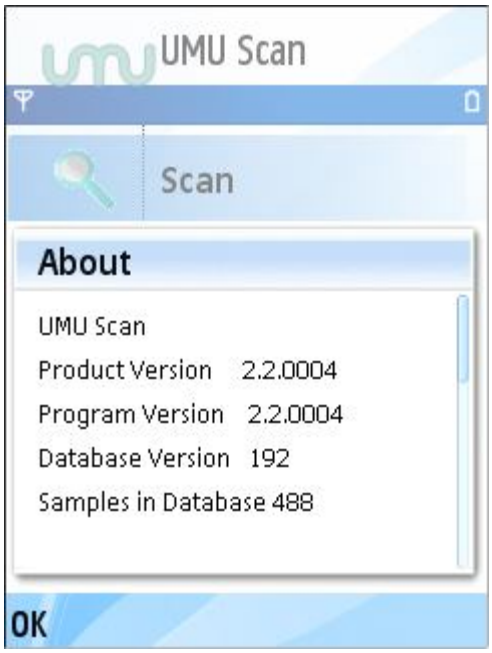

Figure 9: About screen

Status

For information about when the last scan was performed and if an update is due choose Status from the main menu.

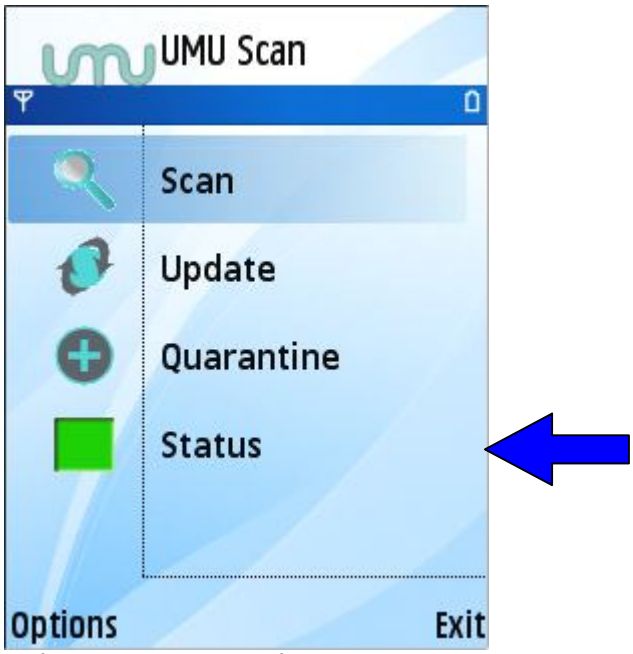

Figure 10: Status on the menu screen

Green indicates that both active scan and scan prompts are enabled, update prompts are enabled, a scan has run recently, and the program is up to date.
Amber indicates that scan prompts are disabled or it has been over a week since the last update or it has been over two weeks since the last scan.
Red indicates that active scan is disabled, or it has been more than two weeks since the last update, or the action on detection is set to “Log only”.

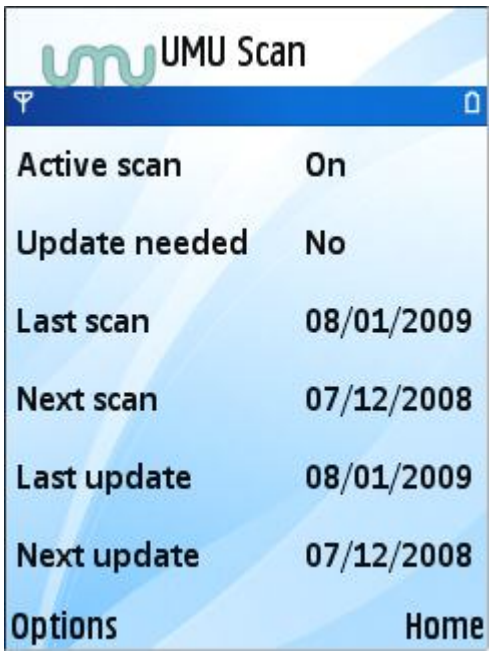

Figure 11: Status screen

Scanning

On the main menu screen choose the Scan option and the scan will start.

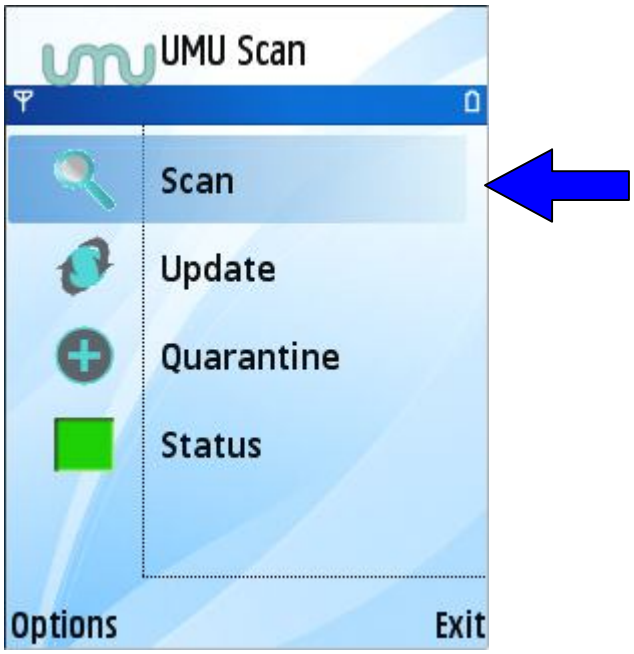

Figure 12: Scan option

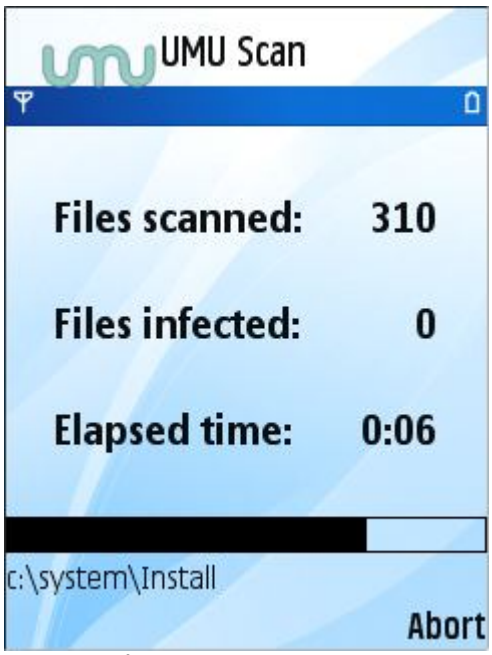

Figure 13: Scan screen

If any viruses are found during the scan, they are automatically quarantined.
If you wish to abort the scan, click on the Abort button. You will be asked whether you are sure you want to abort the scan. If you do not want to abort, choose No and the scan will continue to the end as normal. If you do want to abort, choose Yes and the scan will stop. When the scan completes or is aborted, the scan report screen appears.

Figure 14: Scan report screen

Press Home to return to the main menu screen.

Quarantine

All the viruses found are quarantined in an encrypted file. To view the quarantined files, choose Quarantine in the main menu.

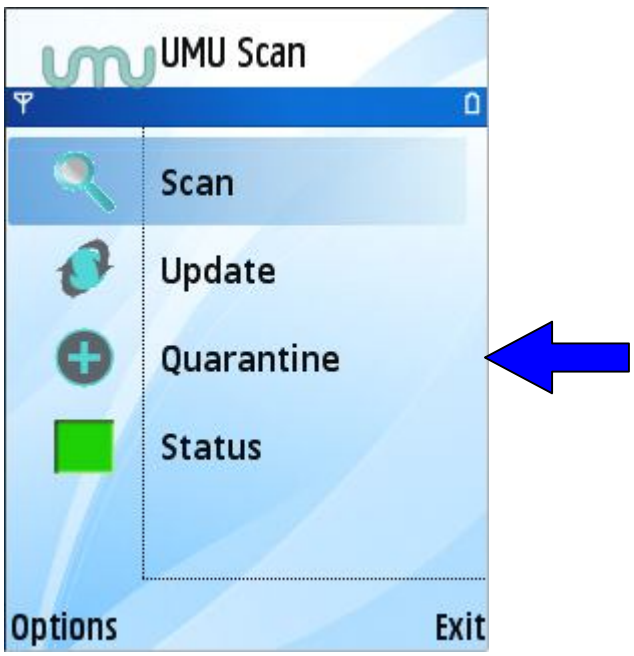

Figure 15: Quarantine option

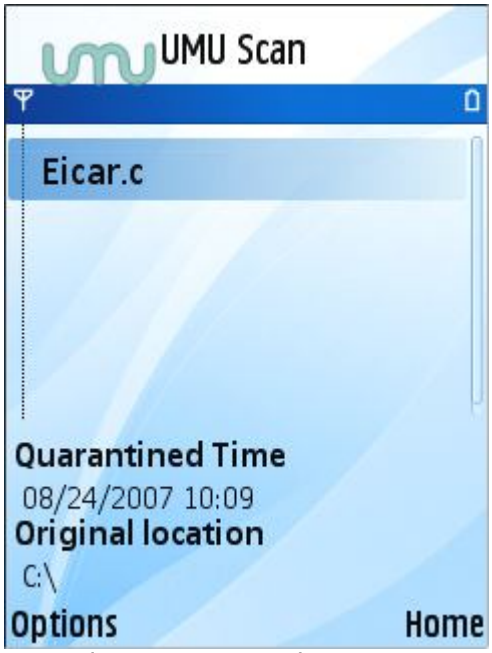

Figure 16: Quarantine screen

To delete quarantined viruses, select the virus, choose Options, and then Delete. To delete all quarantined viruses, choose Options, and then Empty.
To restore quarantined viruses, select the virus, choose Options, and then Restore.
Once you have restored or deleted the viruses you require, choose Home and return to the main menu screen.

Updates

To update the program and virus definitions, choose the Update icon on the main menu screen.

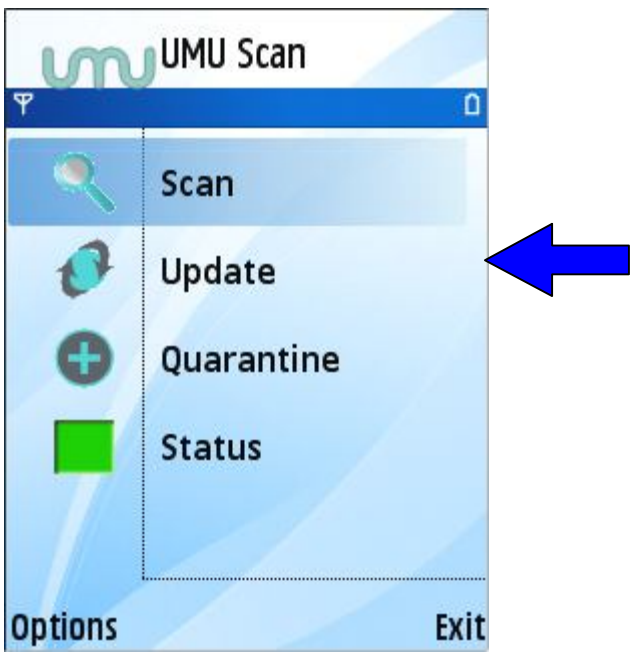

Figure 17: Update option

You will be asked if the program should check for an update on the internet. Choose Yes to update and No to return to UMU Scan.

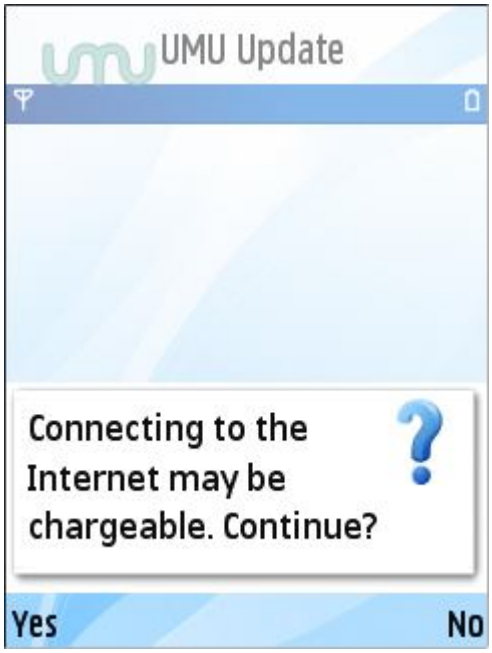

Figure 18: Update pop up

Update will then ask you which access point you wish to use, if the phone is offline or no access points are available you will have to try again when they are available.
If this is the first time you have updated, you will be asked to enter your product key. This was provided when you purchased the product. You will need to enter your product key before any updates can be downloaded and installed.
If updates are available, they will be downloaded and you will be asked if you want to install them. If you select Yes, the update will be installed automatically. You can update UMU Scan either using your device's GPRS internet connection or via a wireless LAN connection if your device supports this.

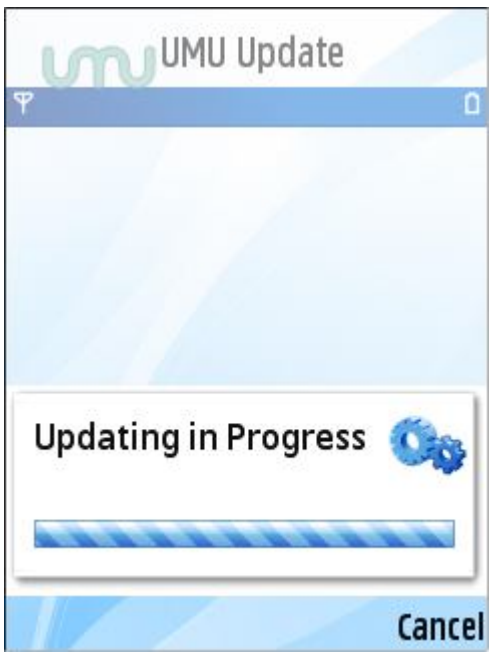

Figure 19: Update screen

Settings

UMU Scan allows you to set reminders to scan and update as well as change many other settings. On the main menu, choose the Options and then Settings

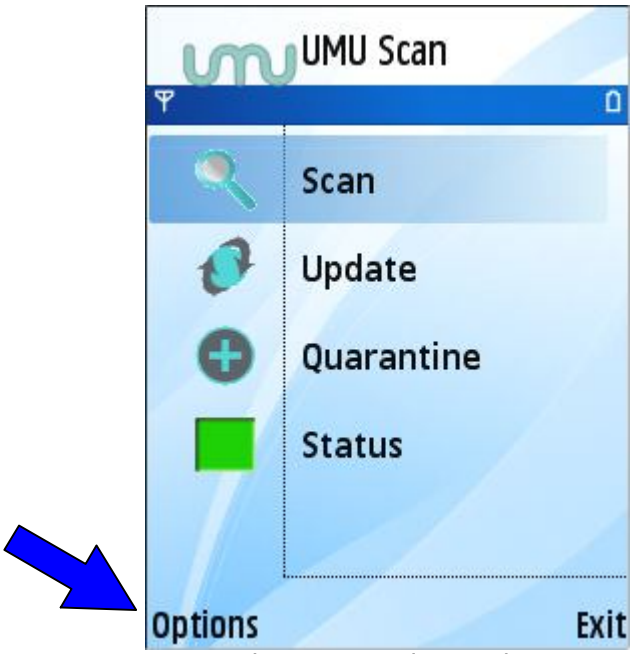

Figure 20: Settings option

This will display the following screen:

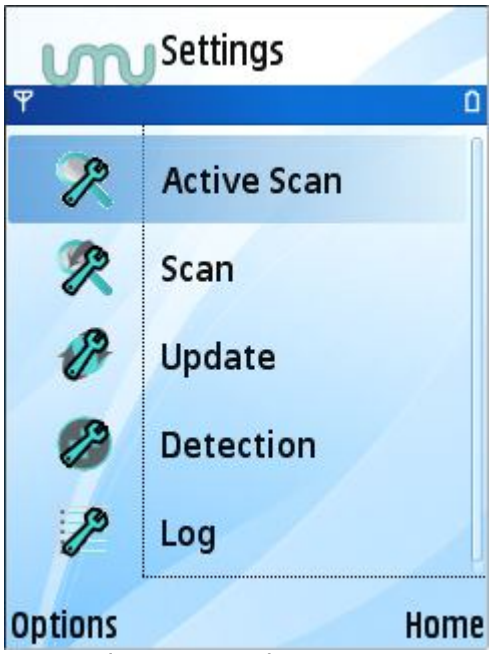

Figure 21: Settings screen

From here, select the area of the program you wish to change. You can also restore all the settings to their default values by selecting Options and then choosing Restore Defaults.

Figure 22: Active scan settings screen

With Active scan enabled, all files on the device are scanned automatically in the background.

It is not recommended that you disable Active scan as this could leave your device at risk from infection.

With “On insertion” selected for Auto scan card whenever a storage card is inserted you will be prompted to scan the card for any infected files.

By default, the options are set as follows:

- **Active scan: Enabled**
- **Auto scan card: On insertion**

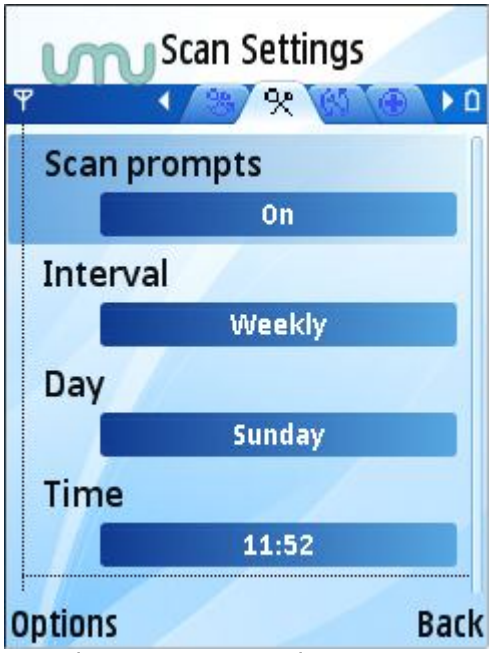

Figure 23: Scan settings screen

If you want to turn off the scheduler so you do not receive prompts to scan, choose off and click Back.

It is not recommended that you turn off the Scan prompts as this could leave your device at risk from infection.

You can set the scheduler to remind you to scan on a daily, weekly or monthly basis. Choose the interval and then choose the day, date and time you would prefer.
Once you have made all the changes you require, click Back and you will be returned to the settings screen.

By default, the options are set as follows:

- **Scan prompts: On**
- **Interval: Weekly**
- **Day: Sunday**

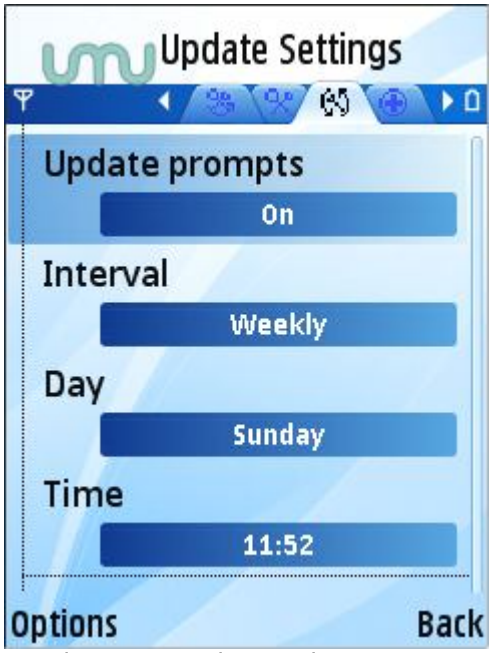

Figure 24: Update settings screen

If you want to turn off the scheduler so you do not receive prompts to update, choose off and click Back.

It is not recommended that you turn off the Update prompts as this could leave your device at risk from infection.

You can set the scheduler to remind you to update on a daily, weekly or monthly basis. Choose the interval and then choose the day, date and time you would prefer.
Once you have made all the changes you require, click Back and you will be returned to the settings screen.

By default, the options are set as follows:

- **Update prompts: On**
- **Interval: Weekly**
- **Day: Sunday**

Figure 25: Detection settings screen

The settings on this screen allow you to specify what will happen when an infected file is detected. An infected file can be quarantined, deleted or simply logged. If quarantine or delete is selected a backup option is available in case the first action cannot be completed.

By default, the options are set as follows:

- **Action: Quarantine**
- **If unable: Delete**

Figure 26: Log settings screen

This settings screen allows you to choose the maximum size for the log file and if it should be displayed starting with the newest or oldest record first.

By default, the options are set as follows:

- **Log file size: Small**
- **Display order: Newest first**

Exiting

In order to exit UMU Scan, click on the exit button in the main menu and the program will close but will continue protecting your device in the background.

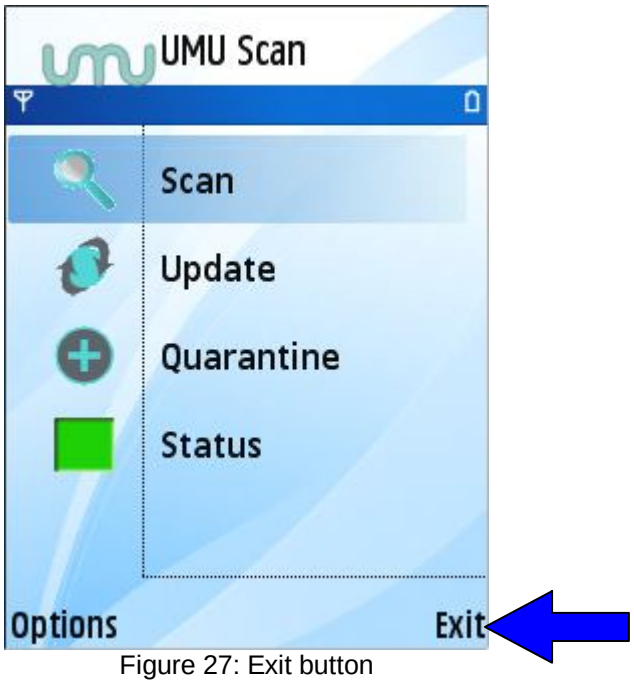

Figure 27: Exit button

Uninstalling

In order to uninstall the UMU Scan program, you need to press the Applications key on your device. Then find and run App. Manager and you will be shown a list of programs you have installed. Select UMU Scan, press Options, and choose Remove. You will be asked to confirm that you want to remove UMU Scan permanently, if you want to remain protected, click No; Click Yes to completely remove UMU Scan from your device. After you have uninstalled UMU Scan, it will no longer protect your device from viruses.

Technical Support

This section gives you instructions on how to find additional technical support.

In program

There is help within the program. From the Options menu select Help and the help page is displayed.

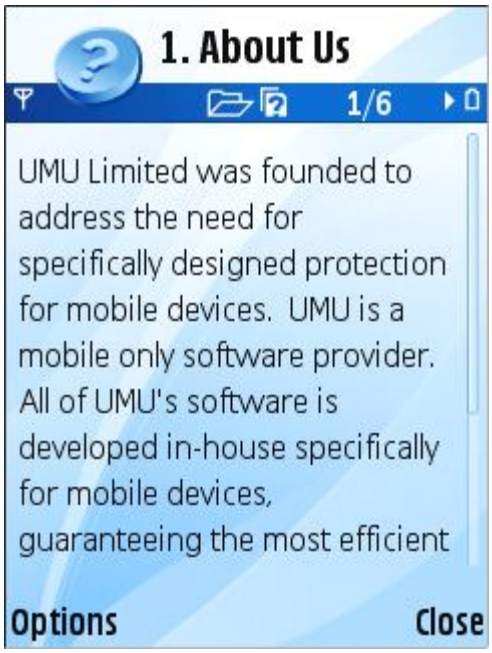
1. About Us
1/6
UMU Limited was founded to address the need for specifically designed protection for mobile devices. UMU is a mobile only software provider. All of UMU's software is developed in-house specifically for mobile devices, guaranteeing the most efficient
Options
Close

Figure 28: Help screen

Frequently Asked Questions

You can view a list of frequently asked questions on the internet at http://www.umuglobal.com/support.php; this site can also be viewed on your device.

Email Support

If you have a question or problem and cannot find a solution in this manual or the FAQ, you can email the support department at support@umuglobal.com.
We recommend that you check the User Manual and the FAQs on the website before contacting the support department with your question as it may have been answered before.

Telephone Support

If you would like to speak to a member of our support department, please telephone:

+44 (0) 1695 735801

Our telephone support line is open Monday to Friday 9am to 5pm GMT/BST except during public or bank holidays.
If you call outside of these hours, you may leave a message and a member of our support department will get back to you.

About UMU Limited

UMU Limited designs and builds innovative security software for mobile devices running Symbian™ and Windows® Mobile operating systems.
We guarantee to deliver fast responses to security alerts and to tackle any threat to your mobile devices with a system that is easy to use, cost effective and will not drain your battery.
We pride ourselves on innovative solutions and customer service, made possible by a dedicated and experienced team of staff.

We are dedicated to mobile security.
Born out of the belief that the AV industry as a whole was failing to offer adequate, focused, and specifically designed protection for mobile devices, UMU Limited was founded in 2004 to address the need for mobile security software. An expanding company based in the North West of England, UMU aims:

- To produce effective, mobile specific security software
- To allow mobile device users to utilise the full capability of their device without fear of infection or intrusion
- To deliver outstanding ease of use
- To deliver swift responses to security alerts

Dependable mobile security solutions are only as good as the research and development that have been expended upon them. With this in mind, UMU is a mobile only software provider so we are not constrained or distracted by desktop PC or server software requirements and footprints.

Friendly, Professional and Approachable
We are an ethical company who have produced the solutions that we feel are important and we have a friendly, professional and approachable team. We have not 'cut down' existing desktop PC or server software for use on mobile devices. All of UMU's software is developed in-house specifically for mobile devices, guaranteeing dedication to the customer's needs and requirements and the most efficient and effective software available.

Visit our website at http://www.umuglobal.com/ to learn more about products, our services, and us.